AMENDMENTS TO THE CLAIMS

Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Currently amended) A method for granting access to a second institution for or via a second device by linking of a first characteristic of a first device and a second characteristic of a second device by a server where the first device is a trusted device and the first characteristic relates to an access legitimization legitimating the first device for accessing a first institution, comprising the steps of:

receiving at the server a request for triggering the following steps ~~a linking between said first device and said second device~~;

selecting a first linking information and a second linking information, the first linking information matching to the second linking information,

sending from the server the first linking information to the first device and the second linking information to the second device,

presenting by the first device the first linking information and by the second device the second linking information, the step of presenting being performed after the step of sending such that the first linking information is output on the first device in parallel to output of the second information on the second device,

entering into the first device an indication of the matching of the first linking information and the second linking information,

based on the entered indication of the matching, sending from the first device to the server a matching confirmation for confirming the matching to the server,

associating the first characteristic and the second characteristic based on the received matching confirmation,

<u>for executing the linking, the server further verifying the access legitimization of the first device,</u>

<u>based on the linking, sending a message from the server for granting access to the second institution</u>.

2. (Previously Presented) The method according to claim 1, wherein the request for linking is a request for authentication and the first device is a trusted device within said communication network, further comprising the step of stating the association by an authentication assertion.

3. (Previously Presented) The method according to claim 2, wherein the authentication assertion is sent for granting access.

4. (Canceled)

5. (Currently amended) The method according to claim <u>1</u> [[4]], wherein the second characteristic comprises an identifier identifying the second device and access to a second institution is granted to or via the second device based on the associating of the first characteristic relating to the access legitimization and the second characteristic comprising the identifier, the second institution being identical to or different from the first institution.

6. (Previously Presented) The method according to claim 1, wherein the first linking information and the second linking information comprise one or more randomly generated symbols.

7. (Previously Presented) The method according to claim 1, wherein the first linking information is identical to the second linking information.

8. (Previously Presented) The method according to claim 1, wherein the associating is based on a verification for correctness of confirmation data entered into the first device.

9. (Previously Presented) The method according to claim 8, wherein the entered confirmation data comprises at least one of

(a) a Personal Identification Number,

(b) a password,

(c) an indication for additional information being presented in parallel to the first linking information or second linking information, the additional information being distinguishable from the first linking information and the second linking information, and

(d) data being computed on the base of the first linking information and/or the second linking information.

10. (Currently amended) A server ~~usable~~ for granting access to a second institution for or via a second device by linking of a first characteristic of a first device and a second characteristic of a second device the first device being a trusted device and the first characteristic relating to an access legitimization legitimating the first device for accessing a first institution, the server comprising:

a receiving unit for receiving messages,

a transmitting unit for sending messages, and

a processing unit for processing messages and information,

wherein the receiving unit is adapted to receive a request for linking, the processing unit is adapted to be triggered by the received request for linking and to select a first linking information and a second linking information, the first linking information matching to the second linking information, the transmission unit is adapted to send the first linking information to the first device and the second linking information to the second device such that the first linking information is output on the first device in parallel to output of the second linking information on the second device, the receiving unit is adapted to receive a matching confirmation from the first device, the matching confirmation confirming to the processing unit the matching of the first linking

information presented by the first device and the second linking information presented by the second device, and the processing unit is adapted to execute an associating of the first characteristic and the second characteristic based on the received matching confirmation, and for executing the linking, to further verify the access legitimization of the first device, and, based on the linking, to send via the transmission unit a message for granting access to the second institution.

11. (Previously Presented) The server according to claim 10, wherein the server is used for authentication, the request for linking is a request for authentication and the first device is a trusted device, the processing unit being further adapted to state the association by an authentication assertion.

12. (Previously Presented) The server according to claim 11, wherein the transmission unit is adapted to send the authentication assertion for granting access.

13. (Canceled)

14. (Currently amended) The server according to claim 10 [[13]], wherein the second characteristic comprises an identifier identifying the second device and, based on the associating of the first characteristic relating to the access legitimization and the second characteristic comprising the identifier, the processing unit is adapted to generate an access assertion for granting to or via the second device access to a second institution being identical or different from the first institution, and the transmission unit is adapted to send the access assertion to the second device or the second institution or to an entity supporting the second device or the second institution for granting access.

15. (Previously Presented) The server according to claim 10, wherein the processing unit is adapted to select the first linking information and the second linking information to comprise one or more randomly generated symbols.

16. (Previously Presented) The server according to claim 10, wherein the processing unit is adapted to select the first linking information being identical to the second linking information.

17. (Previously Presented) The server according to claim 10, wherein the processing unit is adapted to execute the associating of the first characteristic and the second characteristic based on a verification for correctness of confirmation data entered into the first device.

18. (Currently amended) A ~~computer program usable for~~ readable medium having stored thereon a plurality of instructions including instructions which, when executed by a processor, cause the processor to perform the steps of a method for granting access to a second institution for or via a second device by linking of a first characteristic of a first device and a second characteristic of a second device the first device being a trusted device and the first characteristic relating to an access legitimization legitimating the first device for accessing a first institution, ~~the computer program being loadable into a processing unit of a server, wherein~~ the ~~computer program~~ ~~comprises~~ comprising of:

responsive to a request received at the server, triggering the following steps: ~~code adapted to be triggered by a request for linking, to select~~

selecting a first linking information and a second linking information, the first linking information matching to the second linking information,

initializing ~~to initialize~~ a sending of the first linking information to the first device and a sending of the second linking information to the second device such that the first linking information is output on the first device in parallel to output of the second linking information on the second device, and

executing ~~to execute~~ an associating of the first characteristic and the second characteristic based on a matching confirmation received from the first device, the matching confirmation confirming ~~to the computer program~~ the matching of the first linking information presented by the first device and the second linking information presented by the second device, and for executing the linking.

further verifying the access legitimization of the first device, and, based on the linking, initializing a sending of a message for granting access to the second institution.

19. (Currently amended) The computer ~~program~~ readable medium of claim 18 wherein the association is further based on a verification for correctness of confirmation data entered into the first device.

20. (Currently amended) The computer ~~program~~ readable medium of claim 19 wherein said entered confirmation data includes a password.